PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-023331
(43)Date of publication of application : 23.01.1996

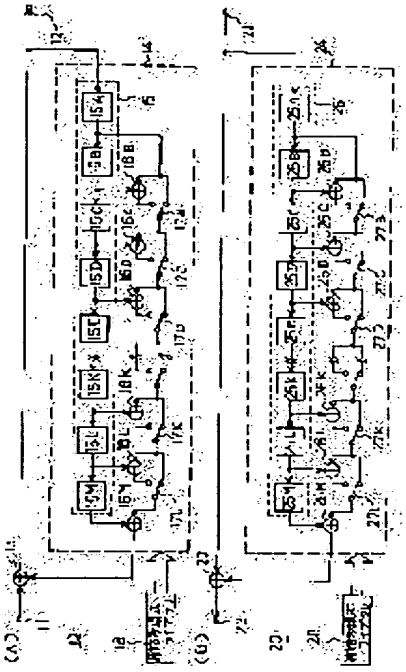
(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00
H04K 1/00

(21)Application number : 06-156307
(22)Date of filing : 07.07.1994

(71)Applicant : MURATA MACH LTD
(72)Inventor : MURAKAMI YASUMICHI
ITO KAZUHITO

(54) METHOD AND DEVICE FOR CIPHERING COMMUNICATION

(57)Abstract:
PURPOSE: To attain ciphering and deciphering with simple configuration by applying self synchronization ciphering to communication information based on a selected irreducible polynomial, sending the to the received information.
CONSTITUTION: A bit string received by a shift register 15 is subject to arithmetic operation at prescribed bits while being shifted sequentially therein and the result is given to an adder 13. The shifting operation is conducted synchronously with an input operation of the bit string to a terminal 11. That is, the ciphering is conducted by dividing a message polynomial representing the received bit string with coefficients in descending order by a ciphering generating polynomial (key). Then the bit string received from an input terminal 21 is given to an adder 23 and a primitive polynomial configuration section 24. The adder 23 receives the bit string from the terminal 21 and the primitive polynomial configuration section 24. An output of the adder 23 is outputted from a terminal 22 as a decoded bit string. That is, a decoding circuit 20 uses the same primitive polynomial as that of a ciphering circuit 10 to decode the ciphered data.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－23331

(43)公開日　平成８年(1996) １月23日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/06				
	9/14				
Ｇ０９Ｃ	1/00		7259－5Ｊ		
Ｈ０４Ｋ	1/00	Ｚ			
				Ｈ０４Ｌ　9/ 02　Ｚ	

審査請求　有　請求項の数６　ＯＬ　（全 13 頁）

(21)出願番号　特願平6－156307

(22)出願日　平成６年(1994) ７月７日

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地

(72)発明者　村上　恭道
京都市伏見区竹田向代町136番地　村田機械株式会社本社工場内

(72)発明者　伊藤　一仁
京都市伏見区竹田向代町136番地　村田機械株式会社本社工場内

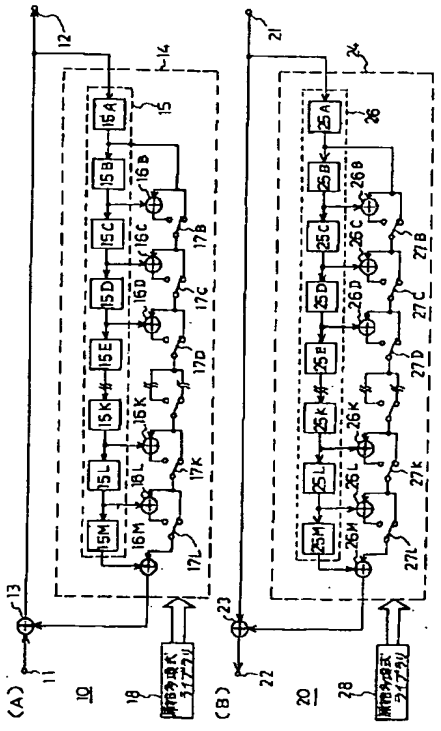
(54)【発明の名称】　暗号化通信方法及び装置

(57)【要約】

【目的】　伝送路上で通信データに欠落を生じ易い通信回線でも、暗号化、復号化が可能な暗号化通信装置及び方法を提供する。

【構成】　複数の既約多項式をもつ自己同期形の暗号化／復号化回路を使用する。暗号化通信に先立ち、送受間で暗号化に使用する既約多項式を選択する。送信側では、選択された既約多項式によって通信情報を暗号化して送信する。受信側では、選択された既約多項式によって受信した通信情報を復号化する。

【効果】　既約多項式そのものを鍵とすることによって、簡易な構成で、欠落データの影響を排除できる。



1

【特許請求の範囲】

【請求項１】　送信局及び受信局に複数の既約多項式を備え、暗号化通信に使用する少なくとも１つの既約多項式を送信局及び受信局で選択し、送信局は選択された既約多項式によって通信情報を自己同期暗号化して送信し、受信局は選択された既約多項式によって受信した通信情報を自己同期復号化することを特徴とする暗号化通信方法。

【請求項２】　請求項１に記載の暗号化通信方法において、前記既約多項式は原始多項式であることを特徴とする暗号化通信方法。

【請求項３】　複数の既約多項式を記憶した記憶手段と、前記記憶手段に記憶された既約多項式から少なくとも１つの既約多項式を選択する選択手段と、前記選択手段に基づき任意の既約多項式を構成する少なくとも１つの既約多項式構成手段と、前記既約多項式構成手段によって構成された既約多項式によって暗号化、復号化を行う自己同期暗号化／復号化手段を備えることを特徴とする暗号化通信装置。

【請求項４】　請求項３に記載の暗号化通信装置において、前記選択手段は乱数発生手段を含むことを特徴とする暗号化通信装置。

【請求項５】　請求項３に記載の暗号化通信装置において、前記選択手段は通信相手局から受信した情報に基づいて既約多項式を選択することを特徴とする暗号化通信装置。

【請求項６】　請求項３乃至５の各々に記載の暗号化通信装置において、前記既約多項式は原始多項式であることを特徴とする暗号化通信装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、デジタルデータ通信に適する暗号化通信方法及び装置に関する。さらに詳しくは、伝送路上で通信データに欠落が生じても使用することが可能な暗号化通信方法及び装置に関する。

【０００２】

【従来の技術】デジタルデータ通信における通信の傍受から通信の秘密を守るために、通信情報を暗号化することが行われている。図８（Ａ）にその一例を示す。端子４１から暗号化前のビット列（平文情報）が入力され、端子４２から暗号化されたビット列（暗号情報）が出力される。４５は１３ビットのシフトレジスタであり、暗号化の鍵（キー）となるビット列が予め格納されている。端子４１から加算器４３へ１ビットのデータが入力される毎に、シフトレジスタ４５のビット列は矢印４９の方向へ１ビットづつシフトされ、１ビットのデータが加算器４３へ入力される。

【０００３】加算器４３は、端子４１とシフトレジスタ４５から入力されたデータを演算（排他的論理和）し、演算結果を暗号情報として端子４２から出力する。シフトレジタ４５の最上位ビット４５Ｍのデータは、加算器４３へ入力されると共に、シフトレジスタ４５の所定位置にある加算器４６と、最下位ビット４５Ａにも入力される。シフトレジスタ４５の内容は（$2^{12}-1$）回のシフトを繰り返す毎に同じ内容となる。

2

【０００４】復号化（解読）する場合には、図７（Ｂ）に示すように、暗号化とは逆の手順をとる。端子５１から入力された暗号化ビット列と、シフトレジスタ５５のビット列は、加算器５３へ入力される。加算器５３の演算結果が復号されたビット列として端子５２から出力される。シフトレジスタ５５には、シフトレジスタ４５と同じビット列（鍵）が予め格納されており、シフトする毎に、シフトレジスタ５５の最上位ビット５５Ｍのデータは、加算器５３へ入力されると共に、シフトレジスタ５５の所定位置にある加算器５６と、最下位ビット５５Ａにも入力される。

【０００５】

【発明が解決しようする課題】しかしながら、上述の方法では、復号の時、伝送路上でビット列に欠落が生じても、シフトレジスタ５６のビット列は、欠落後のビット列に同期してシフトされることになる。欠落の発生以降の暗号化ビット列と、復号化する鍵（シフトレジスタ５６のビット列）にズレが生じることになり、復号することができない。もし、伝送路上でビット列に欠落が生じると、その後の暗号化ビット列を復号できなくなる。

【０００６】デジタルデータ通信には様々な通信手順があり、これらのなかには伝送路上での伝送誤りの訂正や、欠落データの検出・再送を行う誤り訂正機能を備えているものもある。伝送路上での欠落データを回復できる誤り訂正機能を備えた通信手順においては、上述のような暗号化方法を採用することができるが、再送の為により多くの伝送時間を必要としたり、より高度な暗号化、復号化処理を必要とする。本発明の目的は、伝送路上で欠落データが生じても、欠落データの再送が不要であり、簡易な構成で暗号化、復号化が可能な暗号化通信方法及び装置を提供することである。

【０００７】

【課題を解決するための手段】本発明の暗号化通信方法では、送信局及び受信局に複数の既約多項式を備え、暗号化通信に使用する少なくとも１つの既約多項式を送信局及び受信局で選択し、送信局は選択された既約多項式によって通信情報を自己同期暗号化して送信し、受信局は選択された既約多項式によって受信した通信情報を自己同期復号化することを特徴としている。

【０００８】また、本発明の暗号化通信装置では、複数の既約多項式を記憶した記憶手段と、前記記憶手段に記憶された既約多項式から少なくとも１つの既約多項式を選択する選択手段と、前記選択手段に基づき任意の既約多項式を構成する少なくとも１つの既約多項式構成手段と、前記既約多項式構成手段によって構成された既約多

項式によって暗号化、復号化を行う自己同期暗号化／復号化手段を備えることを特徴としている。

【０００９】

【作用】複数の既約多項式を備える自己同期形暗号化／復号化手段をそれぞれ送信機／受信機に備える。暗号化すべきビット列の通信に先立ち、送受間で複数の既約多項式の内から暗号化に使用する少なくとも１つの既約多項式（以下、特定生成多項式と呼ぶ）を選択し、暗号化／復号化手段に特定生成多項式（鍵）を構成する。

【００１０】特定生成多項式が構成された後、送信側は特定生成多項式を使用して送信ビット列を暗号化する。受信側は、特定生成多項式を使用して受信ビット列を復号化する。自己同期型暗号化／復号化手段を使用しているので、伝送路上においてデータの欠落が発生しても、所定ビット後には、欠落データによる影響を排除できる。また、既約多項式に原始多項式を使用することにより、ランダム度が最大のビットシーケンスを得ることができ、効率的な暗号化ができる。

【００１１】

【実施例】図１（Ａ）は、本発明による暗号化回路１０を示した図である。１１は入力端子であり、平文のビット列が入力される。１２は出力端子であり、暗号化されたビット列が出力される。１４は原始多項式構成部、１＊＊３は演算（排他的論理和）を行う加算器であり、加算器１３には、端子１１と原始多項式構成部１４からビット列が入力される。加算器１３の出力は暗号化されたビット列として端子１２から出力されると共に、原始多項式構成部１４にも入力される。

【００１２】次に、原始多項式構成部１４について説明する。原始多項式構成部１４は、１５Ａ～Ｍより成る１３ビットのシフトレジスタ１５、１２個の加算器１６Ｂ～Ｍ、加算器１６Ｂ～Ｌに設けられたスイッチ１７Ｂ～Ｌを備えている。スイッチ１７Ｂ～Ｌは、加算器１６Ｂ～Ｌを有効化又は無効化するためのものである。

【００１３】本実施例では、１２次の生成多項式を使用し、既約多項式に原始多項式を使用している。１２次の生成多項式は、表１に示すように、１４４個の原始多項式を持っている。原始多項式ライブラリ１８は、表１に示された原始多項式番号とこれに対応する原始多項式データを記憶している。原始多項式データの１又は０は各項の有無を示し、（Ｌ～Ｂ）は対応するスイッチ１７を示す。原始多項式構成部１４は、原始多項式ライブラリ１８に基づいて、１４４個の原始多項式から任意の原始多項式を構成できる。

【００１４】

【表１】

原始多項式ライブラリ

原始多項式番号	原始多項式データ $X^{12}+X^{11}+X^{10}+X^{9}+X^{8}+X^{7}+X^{6}+X^{5}+X^{4}+X^{3}+X^{2}+X^{1}+1$												
	（L	K	J	I	H	G	F	E	D	C	B）		
1	1	0	0	0	0	0	1	0	1	0	0	1	1
2	1	0	0	0	0	0	1	1	0	1	0	0	1
3	1	0	0	0	0	0	1	1	1	1	0	1	1
4	1	0	0	0	0	0	1	1	1	1	1	0	1
5	1	0	0	0	0	1	0	0	1	1	0	0	1
・							・						
・							・						
・・						（一部省略）							
・・							・						
・・・							・						
142	1	1	1	1	1	1	0	1	1	1	0	1	1
143	1	1	1	1	1	1	0	1	1	1	1	0	1
144	1	1	1	1	1	1	1	0	0	1	0	0	1

【００１５】例えば、表１にある原始多項式番号１の原始多項式

$X^{12}+X^{6}+X^{4}+X+1$

を構成する場合には、スイッチ１７Ｂ～Ｌのうち、スイッチ１７Ｂ、Ｅ、Ｇを加算器１６Ｂ、Ｅ、Ｇ側に接続して、加算器１６Ｂ、Ｅ、Ｇを有効状態にする。このように、原始多項式データが１になっている項に対応するスイッチ１７Ｂ～Ｌを加算器１７Ｂ～Ｌに接続することによって、任意の原始多項式を構成することができる。

【００１６】加算器１３から出力されたビット列は、端子１２から出力されると共に、シフトレジスタ１５の最下位ビット１５Ａにも入力される。シフトレジスタ１５

へ入力されたビット列は、順次シフトしながら、所定ビットでは演算を行い、加算器１３へ入力される。このシフト動作は、端子１１へのビット列の入力動作と同期して行われる。つまり、入力ビット列を降べきの順の係数で表したメッセージ多項式を、暗号化生成多項式（鍵）で除算することによって、暗号化が行われる。

【００１７】次に、図１（Ｂ）を参照し、暗号文を復号する復号化回路２０について説明する。２１は入力端子であり、暗号化されたビット列が入力される。２２は出力端子であり、復号化されたビット列が出力される。２４は原始多項式構成部、２３は演算（排他的論理和）を行う加算器である。

【００１８】入力端子２１から入力されたビット列は、加算器２３と原始多項式構成部２４へ入力される。加算器２３には、端子２１と原始多項式構成部２４からビット列が入力される。加算器２３の出力は復号化されたビット列として端子２２から出力される。

【００１９】原始多項式構成部２４は、原始多項式構成部１４と同様に、２５Ａ～Ｍより成るシフトレジスタ２５、加算器２６Ｂ～Ｍ、スイッチ２７Ｂ～Ｌから構成されている。復号化回路２０は、暗号化回路１０と同様に、表１に示された原始多項式番号と、原始多項式データを記憶した原始多項式ライブラリ２８を備え、任意の原始多項式を構成することができる。

【００２０】原始多項式構成部２４では、端子２１からのビット列の入力と同期して、シフトレジスタ２５のシフトを行い、加算器２６Ｂ～Ｍ、スイッチ２７Ｂ～Ｌで定義された演算を行う。原始多項式構成部２４から出力されたビット列は、加算器２３へ入力される。

【００２１】復号化回路２０で、暗号化回路１０と同じ原始多項式を使用することにより、暗号化回路１０によって暗号化された暗号文を復号化することができる。複数の原始多項式から、いづれの原始多項式を使用するかは、通信すべきビット列の送信に先立ち、乱数や演算等を利用して、送受信間で取り決めればよい。

【００２２】暗号化回路１０、復号化回路２０では、１２次の原始多項式を使用したので、伝送路上でデータ欠落が生じても１２ビット後には、データ欠落の影響を排除することができる。次数は１２次より多くても、小さくてもよい。一般的には、次数が大きくなるほど、暗号化の鍵が増えることになる。例えば、１３次の原始多項式は６３０個あり、次数を１次大きくするだけで、原始多項式（鍵）の数を飛躍的に増加させることができる。

【００２３】原始多項式はランダム度が最も高く、最も効率的な暗号化を行うことができるが、原始多項式以外の既約多項式も鍵として使用することができる。原始多項式以外の既約多項式を使用すると、多項式の次数を上げることなく、鍵の数を大幅に増加させることができる。また、本実施例では、ハードウェアとしてのレジスタ、加算器、スイッチを用いたが、マイクロコンピュータとソフトウェア（プログラム）によって本発明を構成することも可能である。

【００２４】複数の原始多項式構成部を並列に構成した暗号化回路３０について、図２を参照しながら説明する。暗号化回路１０に対応する箇所には同じ符号を付している。３８は第２原始多項式ライブラリであり、原始多項式ライブラリ１８と同様に原始多項式番号と原始多項式データを含んでいる。３４は第２原始多項式構成部であり、原始多項式構成部１４と同様にレジスタ３５、加算器３６Ｂ～Ｈ、スイッチ３７Ｂ～Ｇを含み、第２原始多項式ライブラリ３８の原始多項式データに基づき、任意の原始多項式を構成することが可能である。

【００２５】原始多項式構成部１４の加算器２６Ｍの出力と、第２原始多項式構成部３４のスイッチ３７Ｇの出力は加算器３６Ｈ１へ入力される。加算器３６Ｈ１の出力とレジスタ３５の最上位ビット３５Ｈの出力は加算器３６Ｈ２へ入力される。加算器３６Ｈ２の出力と入力端子１１からの入力ビット列は、加算器１３へ入力される。加算器１３の出力が暗号化されたビット列として、出力端子１２から出力されると共に、多項式構成回路１４と、第２多項式構成回路３４にも入力される。

【００２６】第２原始多項式構成部３４の次数は７次であるが、原始多項式構成部１４の次数と異なれば大きくても、小さくてもよい。いま、暗号化に使用する２つの原始多項式の次数をそれぞれm，ｎとすると、m，ｎは（$2^{m}-1$）と（$2^{n}-1$）が互いに素であるように設定するのが望ましい。

【００２７】暗号化回路３０のように、次数の異なる複数の多項式構成部を並列に構成することにより、各々の原始多項式の次数は低くても、実質的には大きな次数の原始多項式を使用した場合と同じ効果を得ることができる。また、複数の多項式の内の最大次数ビット後に、欠落データの影響を排除することができる。例えば、暗号化回路３０のように１２次と７次の原始多項式を使用している場合には、欠落データの発生後、１２ビット後に欠落データの影響を排除することができる。つまり、欠落データの影響を排除するために必要なビット数を増加させることなく、暗号化の鍵を増やすことができる。

【００２８】暗号化回路３０で暗号化された暗号文を復号するには、暗号化回路３０と同様に、復号化回路２０に複数の原始多項式構成部を構成すればよく、詳細な説明は省略する。

【００２９】次に、上述の暗号化回路１０、復号化回路２０を用いたデジタル無線電話機８０について、図３を参照しながら説明する。６１はマイクロホンであり、アナログ音声信号をＡ／Ｄコンバータ６２へ出力する。Ａ／Ｄコンバータ６２は、アナログ音声信号を、デジタル音声データへ変換し、音声圧縮符号化回路６３へ出力する。音声圧縮符号化回路６３は、デジタル音声データのデータ量を圧縮し、暗号化回路１０へ出力する。

【００３０】暗号化回路１０は、原始多項式に基づいて、圧縮されたデジタル音声データを暗号化して、Ｄ／Ａコンバータ６４へ出力する。また、制御部８１からの制御データも、Ｄ／Ａコンバータ６４へ出力される。制御部８１は、通信相手局との通信回線（周波数）の割り当て、接続、開放等を行うための制御データの解析、生成を行う。また、制御部８１は、複数の原始多項式から任意の原始多項式（特定多項式）を選ぶための乱数発生部８２を備えている。

【００３１】Ｄ／Ａコンバータ６４は、デジタルデータを高周波変調できるように、アナログ信号に変換し、高周波送信部６５へ出力する。高周波送信部６５は、アナログ信号を変調してアンテナ８７から高周波を出力する。８６は、送受信でアンテナを共用するためのデュプレクサである。８３は操作部、８４は表示部、８５はブザーである。

【００３２】高周波受信部７５は、アンテナ８７で受信した高周波信号を復調し、Ａ／Ｄコンバータ７４へ出力する。Ａ／Ｄコンバータ７４は、復調されたアナログ信号をデジタル化して、等化処理等を行い、ビット列として、復号化回路２０へ出力する。また、ビット列の一部は制御部８１へ出力される。復号化回路２０は、原始多項式に基づいて、暗号を復号化し、音声圧縮復号化回路７３へ出力する。

【００３３】音声圧縮復号化回路７３は、圧縮符号化されたデジタル音声データを復号化することによって、デジタル音声データを復元し、Ｄ／Ａコンバータ７２へ出力する。Ｄ／Ａコンバータ７２は、デジタル音声データをアナログ音声信号へ変換して、スピーカー７１から出力する。

【００３４】通信時の手順について、図４を参照しながら説明する。通信相手局は、本実施例のデジタル無線電話機８０と同等のものであってもよいし、複数のデジタル無線電話機を一元的に管理する移動通信システムにおける基地局であってもよい。まず、使用者によってデジタル無線電話機８０の操作部８３で所定の操作が行われると、相手局の呼び出し、通話回線の設定を行う（Ｓ１）。

【００３５】次に、乱数発生部８２で乱数を発生させ、乱数に基づいて、暗号化に使用する原始多項式を示す原始多項式番号を選択する。原始多項式番号は、制御データの一部として、通話相手局へも送信される。暗号化回路１０は、選択された原始多項式番号に基づき、原始多項式ライブラリ１８から、原始多項式データを取り出し、スイッチ１７Ｂ～Ｌを操作して原始多項式を構成する（Ｓ２）。原始多項式を選択するために、乱数以外の方法を用いることも可能である。

【００３６】原始多項式の構成が完了すると、通話を開始することができる（Ｓ３）。マイクロホン６１から入力されたアナログ音声信号は、デジタル化、圧縮符号化、そして、暗号化された後、通話相手局へ送信される。通話が終了すれば、通信回線を開放し、通信を終了する（Ｓ４）。

【００３７】本実施例と同じ構成のデジタル無線電話機８０が、被呼側になった場合について説明する。制御部８１が、自局の呼び出しを検出すると、ブザー８５を鳴動させる。ブザーに気付いた利用者が操作部８３の所定のキー（不図示）を操作すると、デジタル無線電話機８０は、着信への応答を行い、通話回線の設定を行う（Ｓ１）。

【００３８】その後、暗号化に使用する原始多項式を示す原始多項式番号を受信すると、復号化回路２０は、原始多項式ライブラリ２８から、原始多項式データを取り出し、スイッチ２７Ｂ～Ｌを操作して、原始多項式を構成する（Ｓ２）。通話が開始されると、高周波受信部７５で受信され、Ａ／Ｄ変換されたデジタル音声データは、復号化回路２０で復号された後、圧縮復号化、アナログ化されてスピーカー７１から出力される（Ｓ３）。通話が終了すれば、通信回線を開放し、通信を終了する（Ｓ４）。

【００３９】上述のデジタル無線電話機８０では、暗号化に使用する原始多項式を選択するために、発呼側で乱数によって原始多項式番号を選択し、被呼側へ原始多項式番号を送信している。原始多項式の選択は、次のように行うことも可能である。

(1) 被呼側のデジタル無線電話機で乱数によって原始多項式番号を選択し、発呼側へ送信すること。

【００４０】(2) 回線接続時に、発呼側、被呼側の電話番号を互いに交換し、いづれか、もしくは、両方に含まれている電話番号と、所定の演算式を使用して原始多項式を選択し、原始多項式を構成し、暗号化通信を行う。演算式が秘密にされていれば、２重の暗号化ができる。

(3) 符号化回路３０を使用した場合には、複数の原始多項式を選択する必要があるが、上述の方法を組み合わせて使用することもできる。

【００４１】次に、前述の暗号化回路１０、復号化回路２０を用いたファクシミリ装置１００について、図５を参照しながら説明する。読取部１０１は、文字や図形等の画像をＣＣＤ等の光電変換素子、バイナリコンバータ等を用いて、デジタル画像データに変換し、冗長度圧縮符号化回路１０２へ出力する。冗長度圧縮符号化回路１０２は、デジタル画像データをＭＨ方式、ＭＲ方式等により冗長度圧縮符号化し、暗号化回路１０へ出力する。

【００４２】暗号化回路１０は、冗長度圧縮符号化された画像データを暗号化して、モデム１０３へ出力する。モデム１０３はデジタルデータを、電話回線Ｌで送信できるように変調したり、電話回線Ｌから受信したアナログ信号を復調する他、通信手順信号の生成、検出を行う。回線制御装置（ＮＣＵ）１０４は、電話回線Ｌとモデム１０３又は付属電話機１０５との接続、開放を行

う。

【００４３】電話回線Ｌを通じて通信相手ファクシミリ装置から受信したアナログ信号は、モデム１０３でデジタルデータに復調され、復号化回路２０へ入力される。復号化回路２０は、暗号化されたデジタルデータを復号して、冗長度圧縮復号化回路１０６へ出力する。冗長度圧縮復号化回路１０６は、暗号を復号されたデジタルデータを冗長度圧縮復号化し、記録部１０７へ出力する。記録部１０７は、電子写真記録方式等によってデジタル画像データを記録紙に印字出力する。

【００４４】１０８はファクシミリ装置１００を操作するためのキー（不図示）等を備えた操作部、１０９はファクシミリ装置１００の動作状態を表示するための表示部、１１０は暗号化に使用する原始多項式を選択するための乱数を発生する乱数発生部である。１１１はファクシミリ装置１００の上述の各部を制御する制御部である。

【００４５】上述のファクシミリ装置１００を被呼側に使用した場合の動作について、図６を参照して説明する。制御部１１１が、局交換器からの呼び出し信号（ＣＩ）を検出すると（Ｓ１１）、制御部１１１はＮＣＵ１０４を制御して、電話回線Ｌとモデム１０３を接続する（Ｓ１２）。その後、所定期間内にＣＮＧ信号を検出できなければ（Ｓ１３）、付属電話機１０５を呼び出し、通話に入るが（Ｓ１４）、所定期間内にＣＮＧを検出すると、ＣＥＤ信号を送出する（Ｓ１５）。

【００４６】暗号化に使用する原始多項式を示す原始多項式番号となる乱数を乱数発生部１１０で発生し（Ｓ１６）、非標準手順を示すＮＳＦ信号と共に、本発明の暗号化通信を行う情報と原始多項式番号を送信する（Ｓ１７）。さらに、ＣＳＩ信号、ＤＩＳ信号を送信（Ｓ１８）した後、ＮＳＳ信号の検出を行う（Ｓ１９）。ＮＳＳ信号を検出することができなければ、発呼局は本発明の暗号化通信が可能でないので、標準手順を実行する（Ｓ２０）。ＮＳＳ信号を検出できれば、発呼局は本発明の暗号化通信が可能なので、ＴＳＩ信号、ＤＣＳ信号を送信（Ｓ２１）した後、原始多項式番号に基づいて、復号化回路２０の原始多項式構成部２４に原始多項式を構成する（Ｓ２２）。

【００４７】モデム１０３のトレーニング（Ｓ２３）が終了後、ＣＦＲ信号を送信し（Ｓ２４）、ＦＡＸメッセージを受信する（Ｓ２５）。受信されたＦＡＸメッセージは復号化回路２０で復号された後、冗長度圧縮復号化回路１０６でイメージデータに復号され、記録部１０７で記録紙へ記録される。通信データの終了を示すＥＯＰ信号を検出すると（Ｓ２６）、ＭＣＦ信号を送信する（Ｓ２７）。その後、ＤＣＮ信号を受信すると（Ｓ２８）、ＮＣＵ１０４を制御して、電話回線Ｌを開放する（Ｓ２９）。

【００４８】次に、上述のファクシミリ装置１００を発呼側に使用した場合の動作について、図７を参照して説明する。ファクシミリ装置１００の使用者が、読取部１０１に原稿を載置した後、操作部１０８から電話番号を入力し、通信キー（不図示）を操作すると、制御部１１１は、ＮＣＵ１０４を制御して電話回線Ｌとモデム１０３を接続して、ＤＴＭＦ信号又はダイヤルパルスを送出する（Ｓ３１）。その後、制御部１１１は、ＣＮＧ信号を送信しながらＣＥＤ信号の検出を行う（Ｓ３２、Ｓ３３）。

【００４９】ＣＥＤ信号を検出すると、ＣＮＧ信号の送出を停止し、ＮＳＦ信号の検出を行う（Ｓ３４）。ＮＳＦ信号が検出されない（標準手順の場合）か、もしくは、検出されても本発明の暗号化通信を示すものでない場合には標準手順を行う（Ｓ３５）。ＮＳＦ信号が検出されるとＣＳＩ信号、ＤＩＳ信号を受信する（Ｓ３６）。ＮＳＦ信号に本発明の暗号化通信を示す情報が含まれている場合には、さらに、暗号化に使用する原始多項式を示す原始多項式番号を検出し、暗号化回路１０に原始多項式を構成する（Ｓ３７）。

【００５０】さらに、本発明の暗号化通信が可能であることを示す情報を含んだＮＳＳ信号、ＴＳＩ信号、ＤＣＳ信号を送信する（Ｓ３８）。モデム１０３のトレーニングを行い（Ｓ３９）、ＣＦＲ信号を受信すると（Ｓ４０）、ＦＡＸメッセージの送信を行う（Ｓ４１）。読取部１０１は、載置された原稿を、順次、走査し、デジタルイメージデータに変換して、冗長度圧縮符号化回路１０２へ出力する。冗長度圧縮符号化回路１０２は、ＭＨ方式等により圧縮符号化して暗号化回路１０へ出力する。

【００５１】暗号化回路１０は、原始多項式構成部１４で構成された原始多項式により、暗号化を行った後、ＦＡＸメッセージをモデム１０３へ出力する。モデム１０３は、ＦＡＸメッセージを変調して、電話回線Ｌへ送出する。原稿の送信が完了すると（Ｓ４２）、ＥＯＰ信号を送信する（Ｓ４３）。ＭＣＦ信号を受信すると（Ｓ４４）、ＤＣＮ信号を送信し（Ｓ４５）、ＮＣＵ１０４を制御して電話回線Ｌを開放する（Ｓ４６）。

【００５２】上述のファクシミリ装置１００では、暗号化に使用する原始多項式を選択するために、被呼側で乱数によって原始多項式番号を選択し、発呼側へ原始多項式番号を送信している。原始多項式の選択は、次のように行うことも可能である。

(1) 発呼側ファクシミリ装置で乱数によって原始多項式番号を選択し、被呼側へ送信すること。

【００５３】(2) ファクシミリ装置１００は付属電話機１０５を備えているので、使用者が付属電話機１０５で相手側ファクシミリ装置の使用者と通話を行い、暗号化に使用する原始多項式の番号を選択し、各々の操作部１０８から原始多項式番号を入力する。発呼側、被呼側の各々のファクシミリ装置１００は、操作部１０８で選択

された原始多項式番号に基づいて原始多項式を構成し、暗号化通信を行う。

【００５４】(3) ファクシミリ手順信号であるＣＳＩ信号、ＴＳＩ信号は、それぞれ被呼側、発呼側ファクシミリ装置の電話番号を含んでいる。発呼側、被呼側の各々のファクシミリ装置１００は、ＣＳＩ信号、ＴＳＩ信号のいづれか、もしくは、両方に含まれている電話番号と、所定の演算式を使用して原始多項式番号を選択し、原始多項式を構成し、暗号化通信を行う。演算式が秘密にされていれば、２重の暗号化ができる。

(3) 符号化回路３０を使用した場合には、複数の原始多項式を選択する必要があるが、上述の方法を組み合わせて使用することもできる。

【発明の効果】

【００５５】本実施例では、通話を行うデジタル無線電話機と画像通信を行うファクシミリ装置について説明したが、発明は伝送路の種類に関係なく適用することができる。また、音声データや画像データに限ることなく、他のデジタルデータ通信にも適用することができる。

【００５６】このように、既約多項式そのものを暗号化／復号化の鍵としているので、通信の最初に暗号化に使用する既約多項式を示す情報を２局間で選択するだけで、暗号化の鍵を設定することができる。また、自己同期式暗号化／復号化手段を使用しているので、伝送路上でビット列に欠落が生じても、所定ビット後には欠落の影響を排除することができる。

【図面の簡単な説明】

【図１】本発明の暗号化通信装置の要部を示す図である。

＊【図２】本発明の暗号化通信装置の要部を示す図である。

【図３】本発明の暗号化通信装置を示すブロック図である。

【図４】本発明の暗号化通信方法を示すフローチャートである。

【図５】本発明の暗号化通信装置を示すブロック図である。

【図６】本発明の暗号化通信方法を示すフローチャートである。

【図７】本発明の暗号化通信方法を示すフローチャートである。

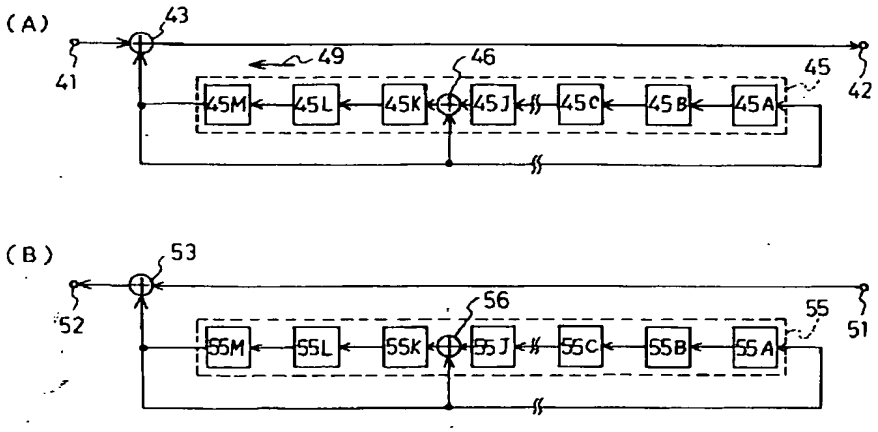
【図８】従来の暗号化回路、復号化回路である。

【符号の説明】

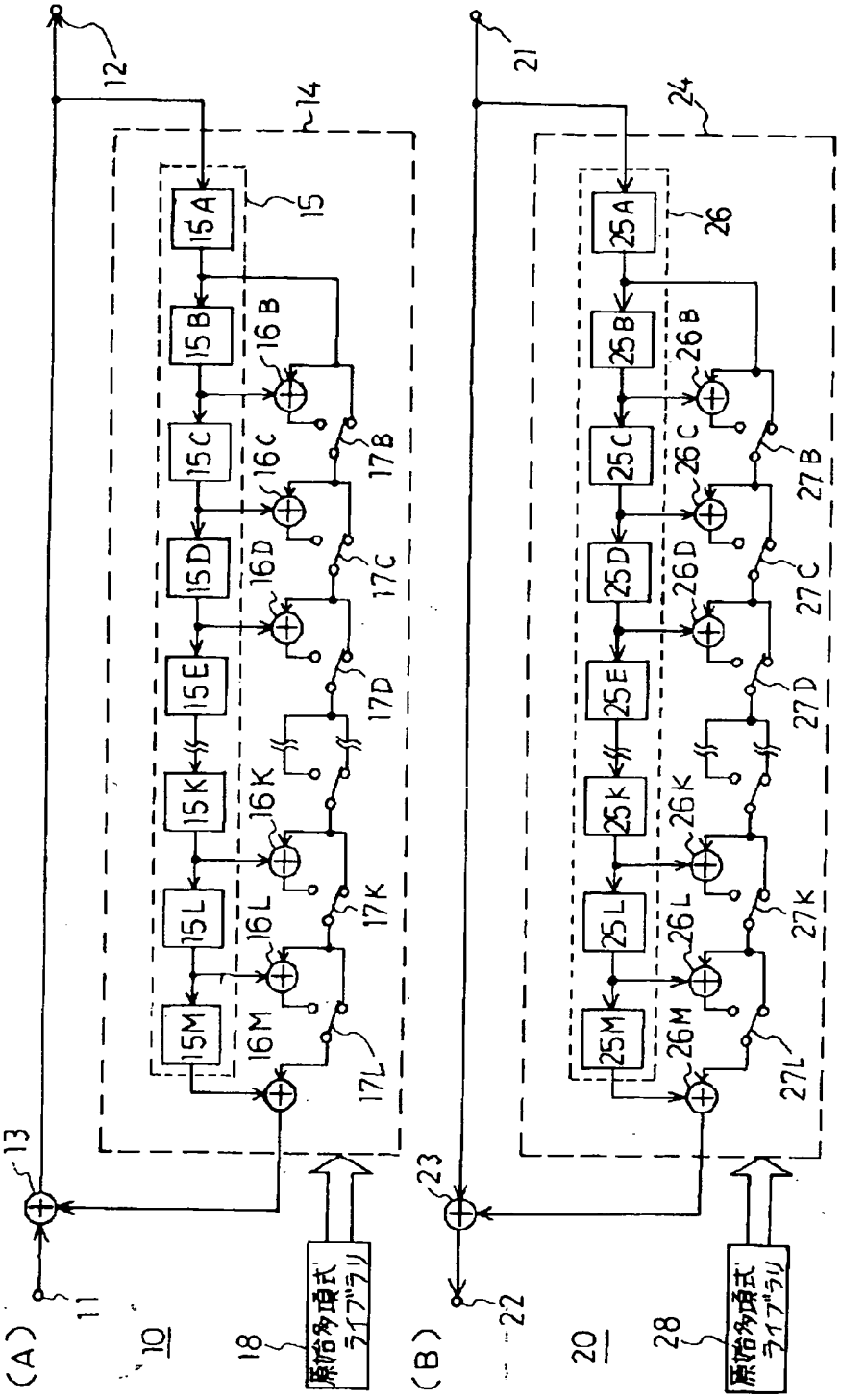
１０，３０	暗号化回路
２０	復号化回路
１１，２１	入力端子
１２，２２	出力端子
１３，２３	加算器
１４，２４，３４	原始多項式構成部
１５，２５，３５	シフトレジスタ
１６Ｂ～Ｍ	加算器
２６Ｂ～Ｍ	加算器
３６Ｂ～Ｈ	加算器
１７Ｂ～Ｌ	スイッチ
２７Ｂ～Ｌ	スイッチ
３７Ｂ～Ｇ	スイッチ
１８，２８，３８	原始多項式ライブラリ

＊

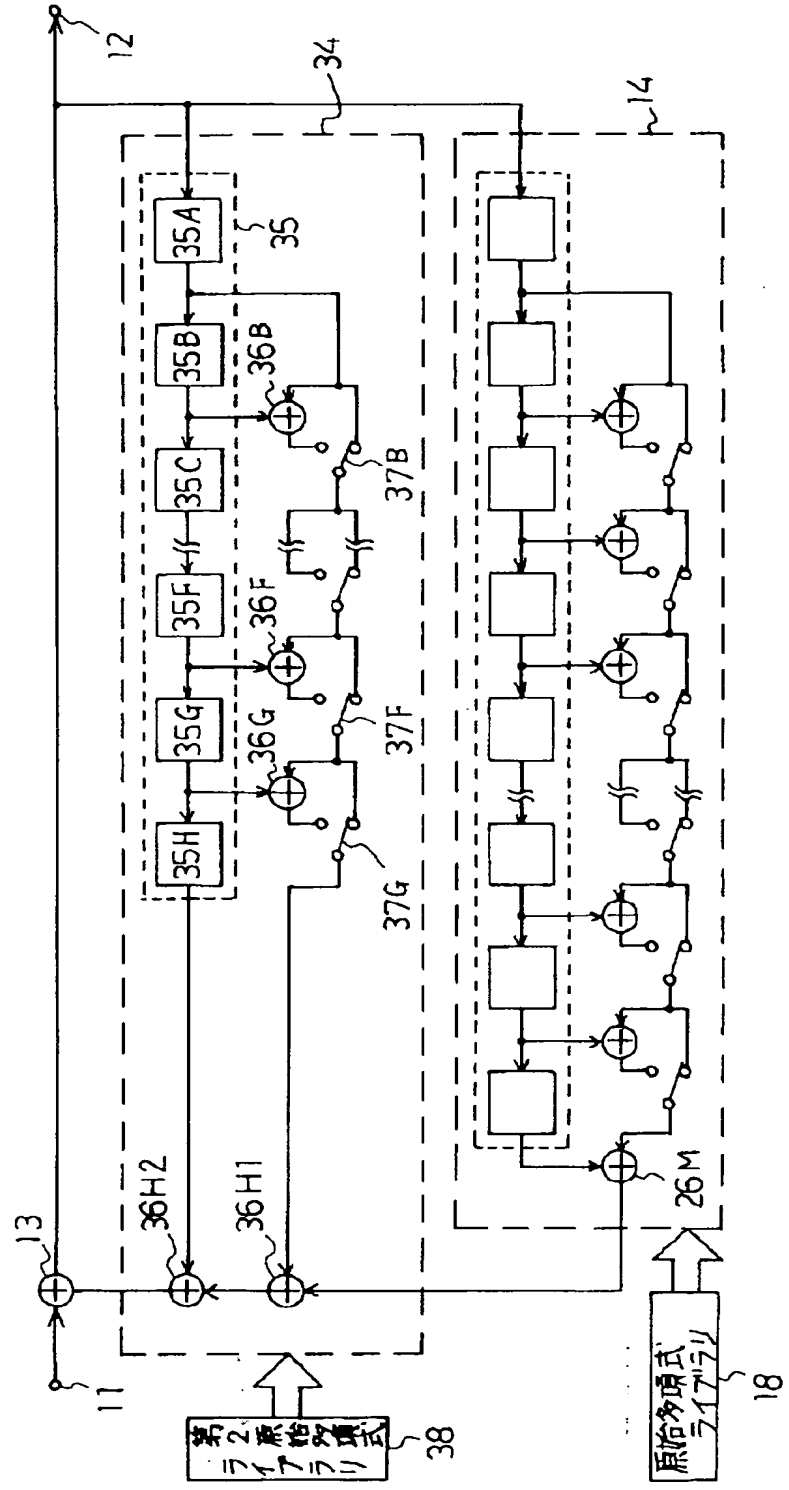
【図８】



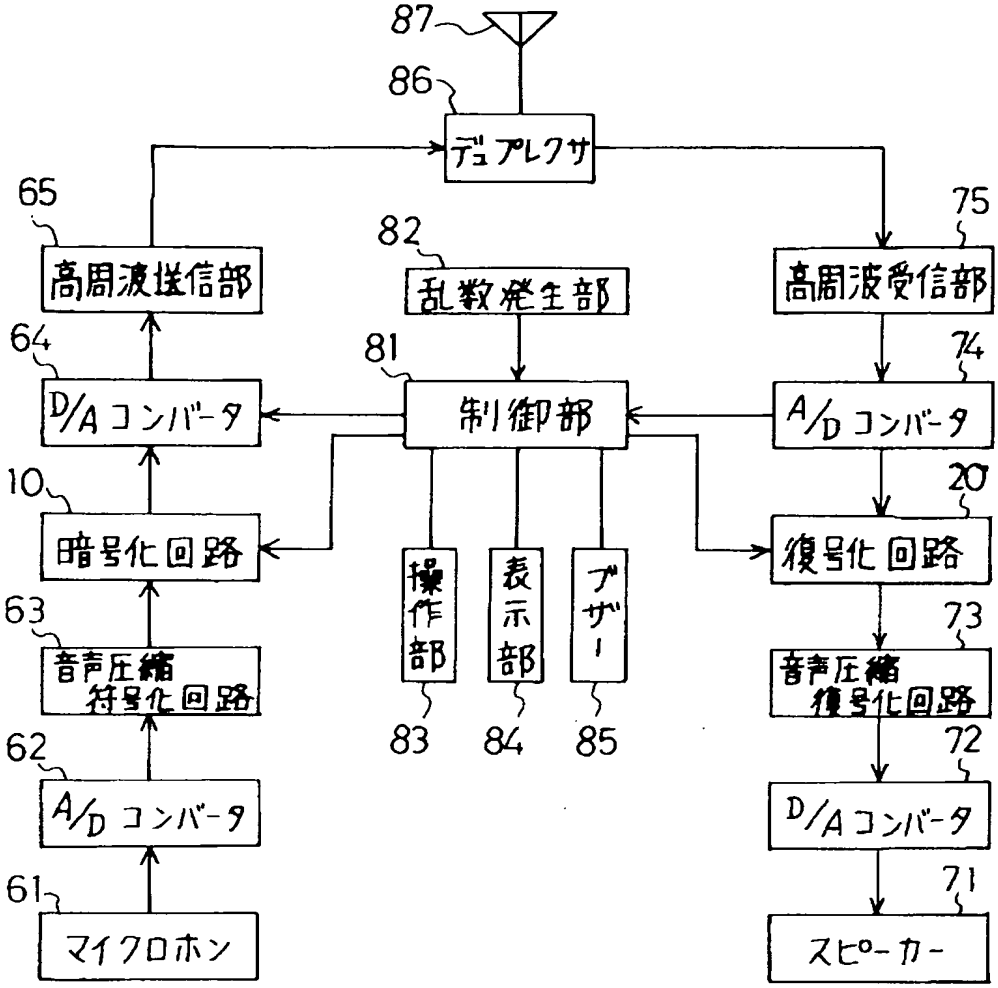
【図１】


(A)
(B)
10
11
12
13
14
15
15A
15B
15C
15D
15E
15K
15L
15M
16B
16C
16D
16K
16L
16M
17B
17C
17D
17K
17L
18
原始多項式ライブラリ
20
21
22
23
24
25A
25B
25C
25D
25E
25K
25L
25M
26
26B
26C
26D
26K
26L
26M
27B
27C
27D
27K
27L
28
原始多項式ライブラリ

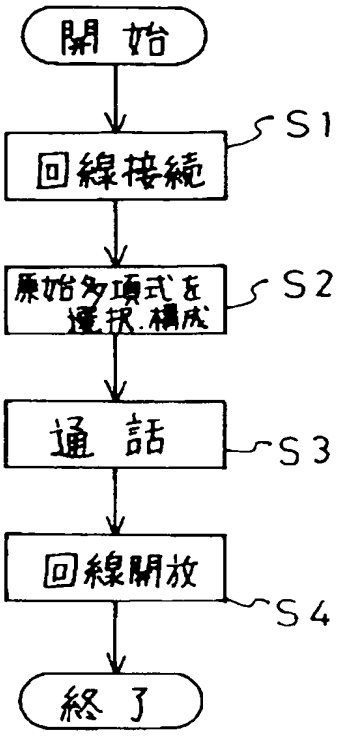
【図２】


12
34
14
35
35A
35B
35C
35F
35G
35H
36B
36F
36G
37B
37F
37G
13
36H2
36H1
26M
30
11
38
18

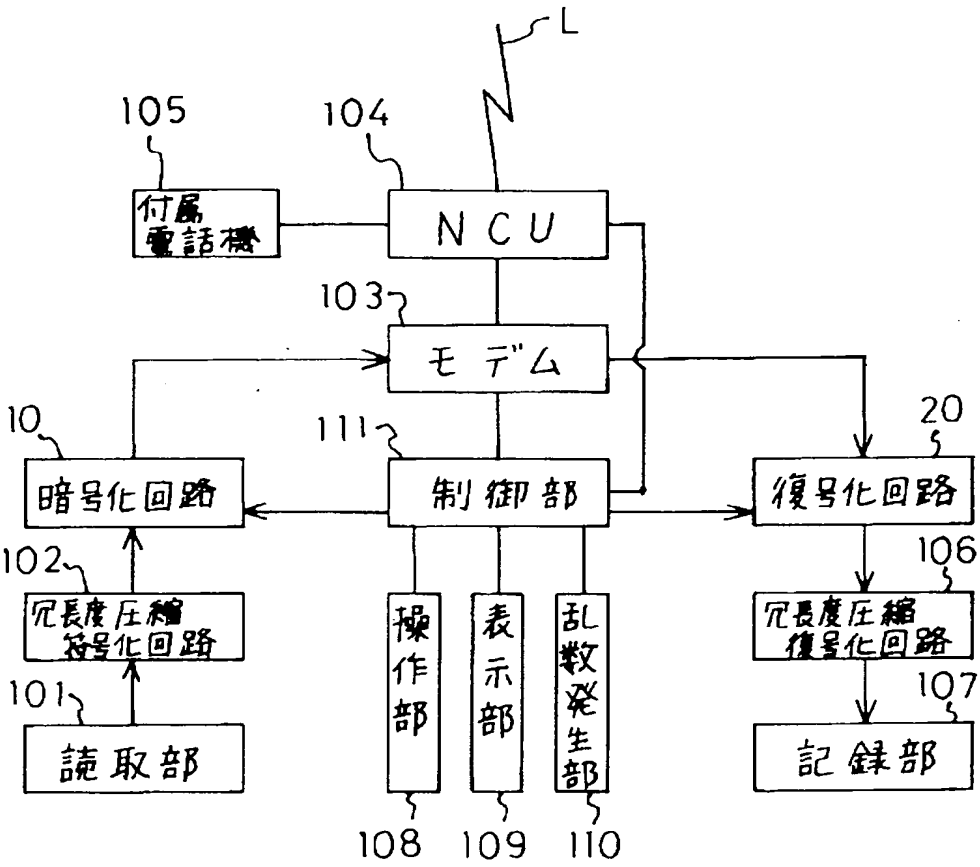
【図３】


87
86
デュプレクサ
65
高周波送信部
64
D/Aコンバータ
10
暗号化回路
63
音声圧縮符号化回路
62
A/Dコンバータ
61
マイクロホン
82
乱数発生部
81
制御部
操作部
表示部
ブザー
83
84
85
75
高周波受信部
74
A/Dコンバータ
20
復号化回路
73
音声圧縮復号化回路
72
D/Aコンバータ
71
スピーカー
80

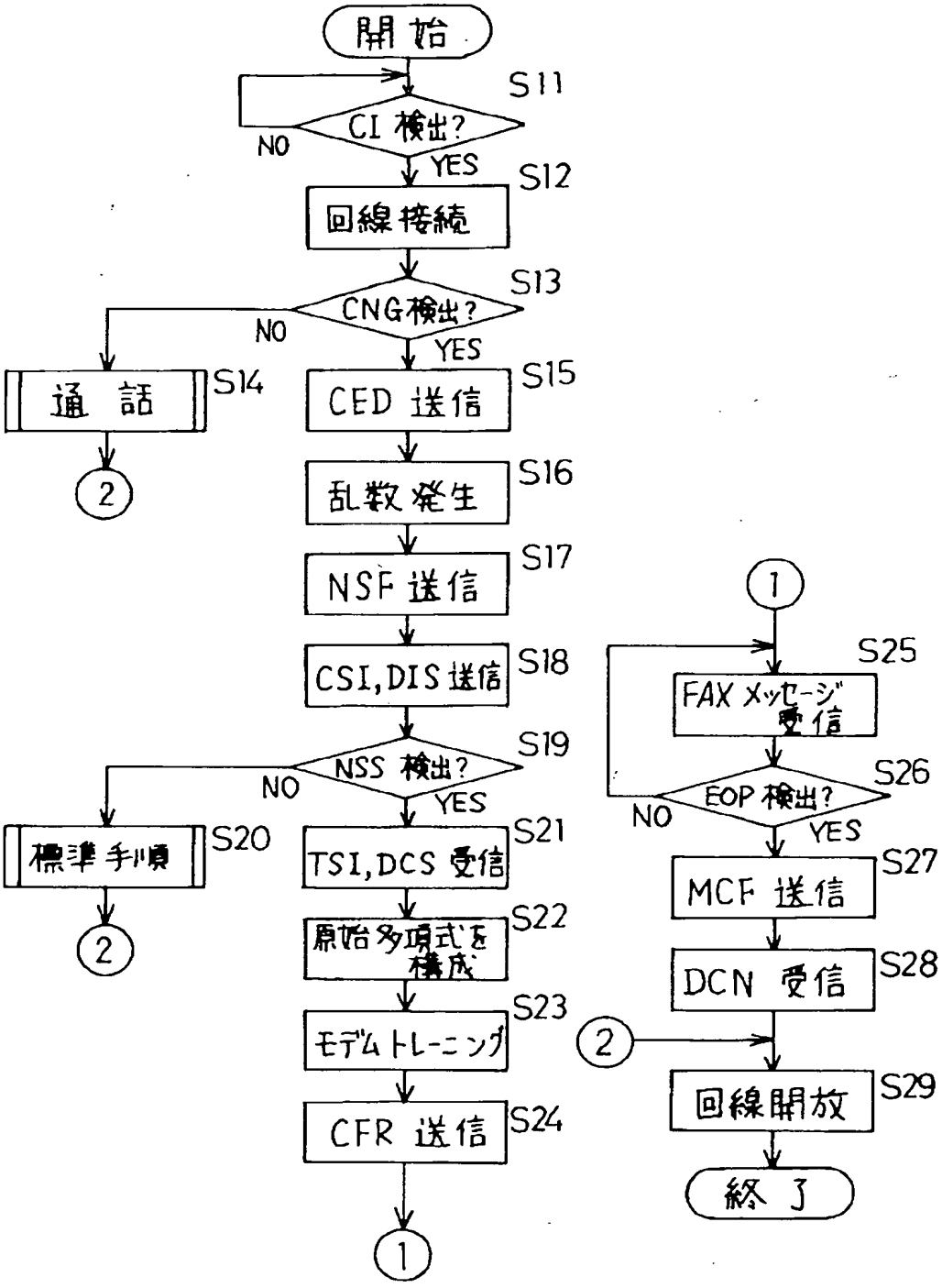
【図４】


開始
回線接続
S1
原始多項式を選択構成
S2
通話
S3
回線開放
S4
終了

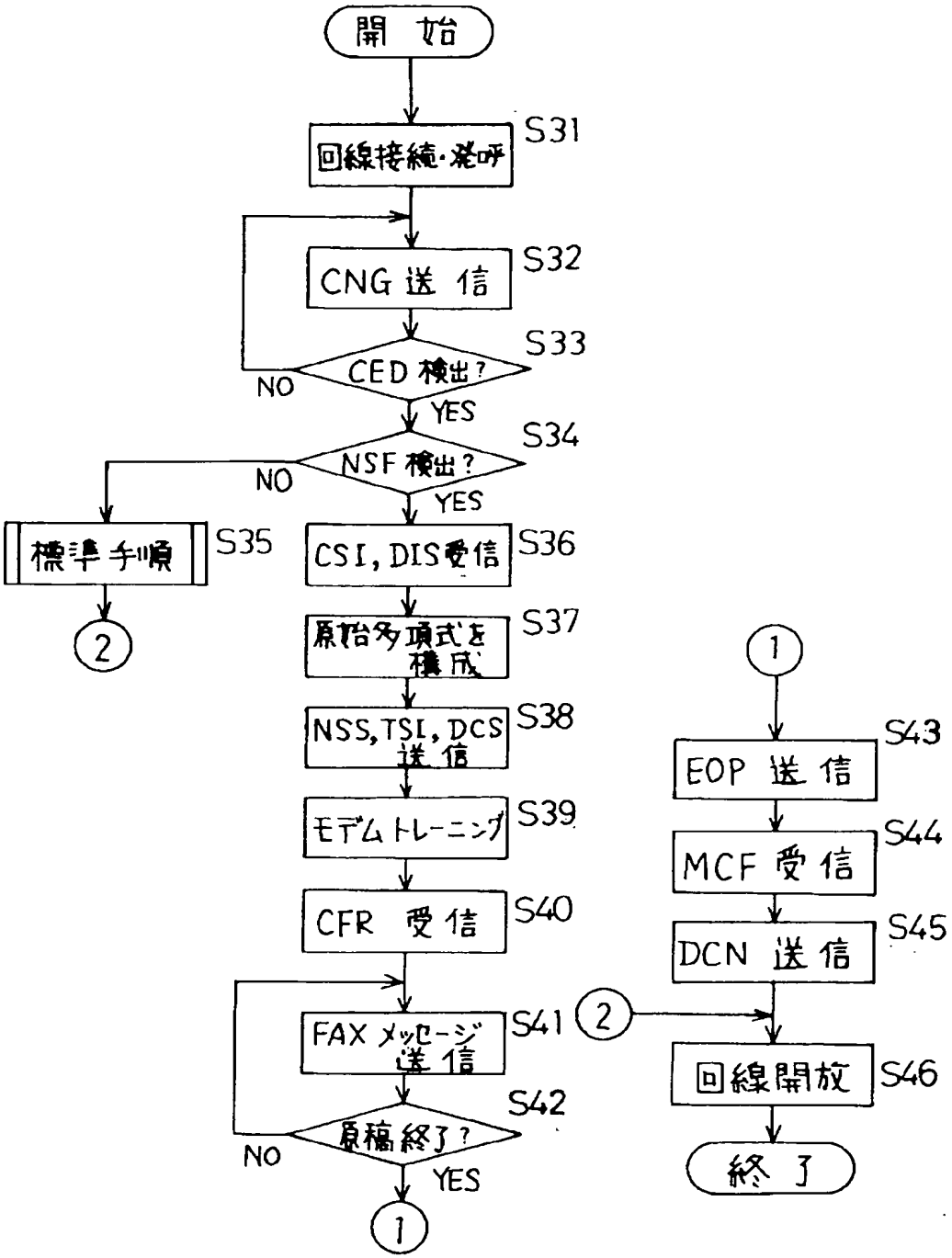
【図５】


L
105
104
付属電話機
NCU
103
モデム
10
111
20
暗号化回路
制御部
復号化回路
102
106
冗長度圧縮符号化回路
操作部
表示部
乱数発生部
冗長度圧縮復号化回路
101
107
読取部
記録部
108
109
110
100

【図６】


開始
S11
CI 検出?
NO
YES
S12
回線接続
S13
CNG検出?
NO
YES
通話
S14
CED 送信
S15
乱数発生
S16
NSF 送信
S17
CSI,DIS送信
S18
NSS 検出?
S19
NO
YES
標準手順
S20
TSI,DCS 受信
S21
原始多項式を構成
S22
モデムトレーニング
S23
CFR 送信
S24
2
1
1
S25
FAX メッセージ受信
S26
EOP 検出?
NO
YES
MCF 送信
S27
DCN 受信
S28
2
回線開放
S29
終了

【図７】


開 始
回線接続・発呼
S31
CNG 送 信
S32
CED 検出?
S33
NO
YES
NSF 検出?
S34
NO
YES
標準手順
S35
CSI, DIS受信
S36
原稿多項式を構成
S37
NSS, TSI, DCS 送 信
S38
モデムトレーニング
S39
CFR 受 信
S40
FAX メッセージ 送 信
S41
原稿終了?
S42
NO
YES
1
2
1
EOP 送 信
S43
MCF 受 信
S44
DCN 送 信
S45
2
回線開放
S46
終 了